Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 09| 2025

Research Article

Received: 25-07-2025| Accepted: 15-08-2025 | Published: 12-09-2025

Decentralized Identity Wallets: Bridging Blockchain and HIPAA Compliance in Healthcare

Sreejith Kaimal

Independent Researcher, USA

Abstract: Decentralized Identification Wallets represent a transformative approach to health care information management, resolving data fragmentation, security weaknesses, and important challenges in limited patient agency. By taking advantage of blockchain technology and cryptographic principles, these systems enable patients to maintain their medical information ownership and control by facilitating safe and selective sharing with healthcare providers. This article examines how to identify identity by implementing ingredients, advanced recovery protocols, and optimized distributed leaders within a HIPAA-analog structure. How can I identify the identity and implement a robust multi-payer compatible member identity system in healthcare? Integration of hybrid storage architecture, zero-knowledge proofs, and smart contract-based consent management creates a strong technical foundation for patient-controlled health records, well-organized administrative procedures, increased border care, and better clinical research. Despite the regulatory challenges related to data modification rights and business associate relations, innovative technical solutions suggest that blockchain technology can co -existence with the healthcare regulatory structure established by providing better security, interoperability, and patient empowerment.

Keywords: Decentralized identity, blockchain healthcare, HIPAA compliance, patient data sovereignty, cryptographic security.

INTRODUCTION

The Paradigm Shift in Healthcare Information Management

Healthcare systems worldwide are experiencing a transformative change from institute-centered to patient-focused data management. Traditional Electronic Health Records (EHR) systems, which digitize medical information, have abolished a model where healthcare providers and insurance companies maintain patient data control. This centralized approach has resulted in significant challenges, including data fragmentation, security weaknesses, and limited patient agency. Studies indicate that despite the rate of 96% EHR adoption between US hospitals, the fragmented healthcare data leads to about $ 342 billion in waste annually, with administrative disability accounting for $ 265 billion of this total. In addition, mismanaged care of fragmented patients contributes an additional contribution of $ 78 billion to unnecessary expenditure each year (HelixBeat, 2025).

The centralized health care information system has consistently demonstrated its weaknesses. According to the Civil Rights (OCR) for the Department of Health and Human Services (HHS) office, 713 major healthcare data violations were reported in 2023, affecting more than 87 million individuals. This represents an increase of 72%in persons affected compared to 2022. The most common type of violation was hacking/IT events (76%), followed by unauthorized access/disclosure (20%), and remaining theft, loss, or improper disposal. Healthcare providers were responsible for 70% of all reported violations, while business partners were responsible for 16%. In particular, 29% of all reported violations include network servers, with the second most common place of information violated on email 23% (Kathrin “Kat” Zaki, *et al.*, 2024).

Despite initiatives like Fast Healthcare Interoperability Resources (FHIR) and Health Level Seven (HL7), interoperability remains an unresolved challenge. According to a comprehensive analysis, the average healthcare provider spends 8–12 hours weekly related to administrative functions related to fragmented data, resulting in an annual productivity loss of approximately $ 27,500 per doctor. The quality of patient care is also suffering, with 44% of patients reporting, they had to repeat the tests due to unavailable results in various providers, while 57% indicated experiencing delay in care due to information exchange problems. These incompetencies contribute to an estimated $ 42 billion that is spent annually on the US healthcare system's inadequate interstitial solutions (HelixBeat, 2025).

Decentralized identification represents a promising solution for these challenges by originally restructuring the relationship between wallet patients and their health data. By taking advantage of the outline of distributed account book technologies, cryptographic principles, and self-confident identity, these systems enable patients to

*Corresponding Author: Sreejith Kaimal

DOI- https://doi.org/10.5281/zenodo.17105992

maintain their medical information ownership and control by facilitating safe and selective sharing with healthcare providers. Preliminary implementation displays significant reforms, with pilot programs, and an administrative overhead related to the identity and record harmony of the patient shows a 67% decrease. Additionally, these systems have demonstrated a 79% decrease in unauthorized disclosure incidents compared to traditional centralized systems, addressing critical concerns highlighted in the OCR's breach reporting (Kathrin “Kat” Zaki, *et al.*, 2024).

This article examines the potential of decentralized identity wallets to revolutionize healthcare information management while maintaining compliance with established regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA).

CRYPTOGRAPHIC FOUNDATIONS FOR HEALTHCARE IDENTITY WALLETS

The security architecture of decentralized identity wallets relies on robust cryptographic principles that enable secure data management while maintaining patient sovereignty. These foundations include hierarchical deterministic wallet structures, advanced recovery mechanisms, and distributed ledger technologies optimized for healthcare applications. Recent security assessments indicate that healthcare data breaches have increased by 55.1% since 2019, with the average cost of a healthcare breach reaching $9.23 million in 2023—the highest across all industries for the eleventh consecutive year (Identity Management Institute).

Hierarchical Deterministic Wallets and BIP39 Implementation

Decentralized identity wallets in healthcare typically implement BIP39 (Bitcoin Improvement Proposal 39) standards, which establish a framework for generating deterministic key pairs from mnemonic seed phrases. This approach provides significant advantages in healthcare contexts. The healthcare industry has experienced over 4,500 data breaches affecting more than 314 million medical records since 2009, with 82% of healthcare organizations reporting at least one cybersecurity incident in the past 24 months. Implementing BIP39-based solutions has demonstrated a 63.7% reduction in successful unauthorized access attempts compared to traditional authentication systems across 17 pilot healthcare organizations (Identity Management Institute).

Recovery mechanisms allow patients to restore access to their medical identity through memorized seed phrases (typically 12 or 24 words), addressing concerns about permanent data loss. A deterministic key derivation system enables multiple public-private key pairs to be generated from a single seed, allowing separate keys for different healthcare relationships while maintaining a unified recovery system. This approach has reduced key management overhead by 78.4% while increasing successful authentication rates by 41.2% in clinical environments. Furthermore, enhanced security is achieved as private keys never leave the patient's device, preventing unauthorized access to sensitive health information through man-in-the-middle attacks or server breaches (Identity Management Institute).

Advanced Recovery Protocols for Healthcare Data

Given the critical nature of healthcare information, decentralized identity wallets often implement Shamir's Secret Sharing (SSS) for enhanced recovery security. This cryptographic technique divides recovery keys into multiple shards, requiring a predetermined threshold of shards for wallet restoration. Implementation of SSS in healthcare identity systems has demonstrated 99.7% recovery success rates compared to 76.8% for traditional account recovery methods across 24 healthcare institutions. Recovery time decreased from an average of 7.2 days to 34 minutes, significantly reducing care disruption during identity recovery scenarios (Minango, J. *et al.*, 2025).

Hedera Hashgraph and Healthcare-Optimized Distributed Ledgers

While many distributed Ledger technologies exist, Hedera Hashgraph has emerged as particularly suitable for healthcare applications due to many characteristics. Performance analysis suggests that Hedera Hashgraph has obtained 10,000+ TPS (transactions per second) compared to 500-800 TPS for Ethereum or lower for other leading blockchain networks in 60 minutes. Energy efficiency is similarly dramatic, with Hedera consuming 0.001 kWh per transaction versus 0.03KwH for Ethereum or Bitcoin's 1156 kWh, particularly important for healthcare systems with sustainability mandates (Minango, J. *et al.*, 2025). The cost of transactions on Hedera Hashgraph is

Publisher: SARC Publisher

0.001$ - 1$ as compared to 0.36$ to 71$ for Ethereum.

Consensus efficiency is achieved through Hashgraph's asynchronous Byzantine Fault Tolerance, which reaches consensus without energy-intensive mining. Regulatory compliance is enhanced through Hedera's governance structure, with data showing 97.3% of healthcare applications implemented on Hedera achieving full HIPAA compliance within 90 days, compared to 46.7% for other DLT platforms. Audit capabilities are maintained through immutable logs of data access and modifications, with 99.9995% event capture accuracy across 2.7 million healthcare transactions in production environments (Minango, J. *et al.*, 2025). These characteristics enable healthcare organizations to implement decentralized identity solutions that satisfy both technical requirements for security and regulatory requirements for accountability, ultimately creating a foundation for truly patient-sovereign healthcare data systems.

Table 1: Cryptographic Foundations for Healthcare Identity Systems (Identity Management Institute; Minango, J. *et al.*, 2025)

Technology Component	Implementation Mechanism	Healthcare Application Benefit
BIP39 Standards	Mnemonic seed phrases	Patient-controlled recovery, reduced permanent data loss
Deterministic Key Derivation	Single seed generating multiple key pairs	Simplified key management with relationship-specific credentials
Shamir's Secret Sharing	Threshold-based key reconstruction	Enhanced recovery security with distributed trust
Hedera Hashgraph	Asynchronous Byzantine Fault Tolerance	High transaction throughput with rapid finality
Immutable Audit Logs	Cryptographically linked event records	Comprehensive accountability with privacy preservation

IMPLEMENTATION FRAMEWORK FOR HIPAA-COMPLIANT DECENTRALIZED IDENTITY

The implementation of a decentralized identity wallet in healthcare requires careful consideration of the existing regulatory structure, especially HIPAA. A comprehensive implementation approach addresses data storage, access controls, consent management, and identity verification. Research indicates that healthcare organizations experience an average of 1.5 data breaches per year, with 89% of healthcare institutions having experienced a data breach in the past two years, costing an average of $9.23 million per incident (Andrew, J. *et al.*, 2023).

Hybrid Data Storage Architecture

To maintain HIPAA compliance while leveraging blockchain advantages, decentralized healthcare identity systems typically employ hybrid storage models. On-chain components include immutable ledger entries that store access permissions, consent records, and cryptographic proofs of data integrity. Recent implementations demonstrate that blockchain-based hybrid architectures reduce unauthorized access attempts by 71.3% while improving data retrieval speeds by 34-57% compared to traditional centralized databases. The hybrid approach separates blockchain components into three distinct layers: the application layer, contract layer, and consensus layer, with healthcare data query efficiency improved by 43.7% through this architectural pattern (Andrew, J. *et al.*, 2023).

Off-chain storage houses actual protected health information (PHI) in encrypted repositories such as IPFS or secure cloud storage, with decryption keys controlled exclusively by the patient. Implementations using this model have shown compliance with HIPAA's technical safeguards in 97.8% of audited cases compared to 76.3% for traditional systems. The separation architecture ensures zero PHI exposure on public networks while maintaining comprehensive audit capabilities, with cross-organizational access controls processing an average of 11,567 daily transactions with 99.99932% accuracy in permission enforcement (Andrew, J. *et al.*, 2023).

Zero-Knowledge Proofs for Minimum Necessary Disclosure

The minimum requirement of HIPAA requires only the required information to be disclosed for specific health care purposes. Zero-knowledge proofs enable verification of claims without disclosing the underlying data. In practical

Publisher: SARC Publisher

applications, ZKPs have been shown to reduce data exposure by up to 98.7% while maintaining verification accuracy of 99.998%. Healthcare organizations implementing ZKP technology report an 82% reduction in data breach surface area and a 73% improvement in patient privacy satisfaction scores (Leslie, R. 2024).

Eligibility verification represents a primary use case, with patients proving insurance coverage without exposing policy details. Research indicates that 38% of healthcare data breaches involve insurance information, with ZKP implementations reducing this exposure risk by 91.7%. Condition verification enables clinicians to confirm relevant medical conditions without accessing complete medical histories, addressing the finding that 67% of healthcare records contain more information than necessary for specific treatments. Additionally, age verification for age-dependent treatments validates eligibility without revealing exact birth dates, protecting demographic data that is involved in 44% of medical identity theft cases (Leslie, R. 2024).

Smart Contract-Based Consent Management

Decentralized identity wallets implement consent management through smart contracts that enforce HIPAA-compliant access controls. Analysis shows that traditional consent mechanisms achieve only 62% compliance with HIPAA documentation requirements, while smart contract implementations achieve 94.3% compliance. These systems enable granular permissions where patients specify exactly which data elements providers can access, with temporal limitations allowing time-restricted access. Purpose limitations further restrict data access to specific clinical needs, with 79% of patients reporting increased trust in healthcare systems using these mechanisms. Revocation processing in traditional systems takes an average of 7.3 days, while blockchain-based consent management executes revocations in an average of 3.2 seconds, significantly enhancing patient control over their health information (Leslie, R. 2024).

Table 2: HIPAA-Compliant Implementation Architecture (Andrew, J. *et al.*, 2023; Leslie, R. 2024)

Architectural Element	Design Approach	Compliance Advantage
Hybrid Storage Model	On-chain permissions with off-chain PHI	Prevention of sensitive data exposure on public networks
Zero-Knowledge Proofs	Verification without data disclosure	Adherence to the minimum necessary principle
Smart Contract Consent	Programmable access control rules	Granular, auditable, patient-directed permissions
Attribute-Based Access	Contextual permission enforcement	Purpose-limited data access with detailed control
Cryptographic Verification	Integrity proofs with selective disclosure	Tamper-evident records with privacy preservation

HEALTHCARE APPLICATIONS AND USE CASES

Decentralized identity wallets enable numerous applications that address existing healthcare challenges while creating new possibilities for patient-centered care delivery and health information exchange. Recent systematic reviews have identified 807 studies addressing blockchain in healthcare, with 32.7% focusing specifically on data management and sharing applications (Mohsan, S. A. H. *et al.*, 2022).

Patient-Controlled Health Records

Decentralized identity wallets enable comprehensive patient control over health records through secure, patient-owned digital repositories. Unified record management systems address significant challenges in current healthcare information ecosystems, where only 14% of healthcare organizations report full interoperability capabilities despite 97% acknowledging its importance. Patient-controlled systems implementing blockchain-based access controls have demonstrated 96.3% successful data retrieval rates compared to 76.8% in traditional health information exchanges. Key implementation challenges include user interface complexity (reported by 73% of participants) and integration with legacy systems (affecting 81% of implementation attempts), though newer solutions incorporating self-sovereign identity principles have reduced these barriers by 41% (Mohsan, S. A. H. *et al.*, 2022).

Selective disclosure capabilities enable patients to share only relevant information through verifiable

Publisher: SARC Publisher

credentials, addressing privacy concerns reported by 87% of patients regarding their health data. Continuous access ensures patients maintain control regardless of provider relationships, resolving a critical limitation in current systems where 63% of patients report difficulty accessing historical records when changing providers. This approach results in measurable improvements, with 43% reduction in duplicate testing, 27% improvement in medication reconciliation accuracy, and 39% increase in preventive care compliance in pilot implementations (Mohsan, S. A. H. *et al.*, 2022).

Decentralized Claims Processing and Prior Authorizations

The administrative burden of healthcare can be substantially reduced through decentralized identity solutions. U.S. healthcare administrative costs reached $812 billion in 2017, representing 34.2% of total healthcare expenditures, with administrative simplification identified as a critical reform target. Automated eligibility verification through blockchain implementations has reduced verification times from an average of 13 minutes to under 30 seconds in clinical settings, while decreasing eligibility-related claim rejections by 37% (AbdelSalam, F. M. 2023).

Streamlined prior authorizations address a significant burden, as physicians currently spend an average of 14.9 hours weekly on administrative tasks, with 34% of this time dedicated to authorization processes. Blockchain-based systems have reduced authorization processing time by 82%, from a mean of 6 days to 26 hours. Direct patient-payer interaction has eliminated an average of 3.4 intermediaries in the claims process, reducing associated administrative costs by 27.3% in pilot implementations (AbdelSalam, F. M. 2023).

Cross-Border and Emergency Healthcare

Decentralized identity wallets provide advantages in scenarios where traditional information exchange is challenging. For international travelers, who collectively make 1.4 billion international trips annually, blockchain-based health credentials have reduced critical treatment delays by 47% and decreased adverse events related to incomplete medical histories by 39%. Emergency access implementations have demonstrated 91% successful information retrieval in simulated crisis scenarios compared to 64% for traditional systems, with access time reduced from 8.7 minutes to 37 seconds on average (AbdelSalam, F. M. 2023).

Clinical Research and Trial Management

Decentralized identity solutions offer promising applications for advancing medical research. Traditional clinical trials face significant challenges, with 86% failing to meet enrollment targets on time and 30% of participants dropping out before completion. Blockchain-based participant recruitment has improved protocol-eligible enrollment by 41% while reducing recruitment costs by 33%. Consent management systems have demonstrated 99.7% verifiability of participant agreements compared to 87.3% in traditional paper-based systems (AbdelSalam, F. M. 2023).

Table 3: Healthcare Applications and Use Cases (Mohsan, S. A. H. *et al.*, 2022; AbdelSalam, F. M. 2023)

Application Domain	Implementation Focus	Patient and Provider Benefits
Patient-Controlled Records	Unified health information repository	Comprehensive health history with selective sharing
Claims Processing	Automated verification and submission	Reduced administrative overhead and faster approvals
Cross-Border Healthcare	Portable, verifiable credentials	Treatment continuity for international travelers
Emergency Access	Rapid, appropriate information retrieval	Critical data availability with privacy protection
Clinical Research	Privacy-preserving participant matching	Enhanced recruitment with controlled data sharing

REGULATORY CHALLENGES AND TECHNICAL SOLUTIONS

While decentralized identification wallets provide compelling benefits, their implementation should navigate complex regulatory requirements, especially about data security, right to access and compliance verification. Recent analysis indicates that the healthcare data affects more than 50 million individuals in 2022. The average cost of of $ 10.1 million is a average brech cost-which exceeds $ 4.35 million cross-industry average (Ramachandran, M. 2024).

Publisher: SARC Publisher

HIPAA Right to Access and Immutable Records

HIPAA grants patients the right to request amendments to their health records, which presents challenges for immutable blockchain systems. A systematic review of 63 blockchain implementations in healthcare identified record immutability as a primary concern in 87% of cases when addressing HIPAA compliance. Technical solutions have emerged to address this regulatory-technical conflict, with append-only record systems showing particular promise. Rather than modifying existing records, corrections are added as new entries with clear references to the original data, maintaining a complete audit trail while satisfying regulatory requirements. Organizations implementing this approach report 93% reduction in amendment processing time and 97% improvement in amendment tracking accuracy (Ramachandran, M. 2024).

Versioning systems provide an alternative solution, with multiple versions of records maintained through cryptographic linking that preserves data integrity while enabling functional amendment capabilities. These systems usually apply characteristic-based access control (ABAC) that successfully balances safety with the purpose, obtaining 99.3% appropriate access provisions while preventing 97.6% unauthorized access efforts during controlled testing. Smart contract governance further enhances compliance through automated processes that ensure viewing systems display the most current information. These technical approaches have demonstrated full compliance with HIPAA amendment provisions in 41 of 42 evaluated implementation scenarios while maintaining the immutability benefits essential to blockchain integrity (Ramachandran, M. 2024).

Business Associate Agreements in Decentralized Environments

HIPAA requires Business Associate Agreements (BAAs) between covered entities and service providers, presenting unique challenges for decentralized systems. In blockchain environments, node operators potentially qualify as business associates under HIPAA regulations, with 78% of healthcare compliance officers expressing uncertainty about BAA implementation in distributed networks. Node operator agreements have emerged as a viable solution, with 11 operational healthcare blockchain networks successfully implementing specialized agreements that satisfy BAA requirements while enabling distributed architecture benefits (Vidals, G. 2025).

Smart contract BAAs represent an innovative approach, with encoded agreements automatically enforcing HIPAA-compliant data handling. These programmable agreements have demonstrated 99.4% successful enforcement of data protection requirements across 14,700 test transactions. Federated governance models establish healthcare-specific blockchain networks with formalized governance ensuring regulatory compliance. The Synaptic Health Alliance and MediLedger represent successful implementations of this approach, with both networks achieving HIPAA compliance certification through comprehensive governance frameworks that address the 18 implementation specifications within the HIPAA Security Rule (Vidals, G. 2025).

Technical Safeguards for HIPAA Security Rule Compliance

Decentralized identity wallets must implement specific technical safeguards to satisfy HIPAA Security Rule requirements. End-to-end encryption PHI ensures safety, receives NIST-compliant encryption for 100% of the data elements protected with allowed blockchain implementation. Biometric authentication increases safety by improving user experience, showing 73% faster access time compared to traditional password systems with implementation data, while maintaining false acceptance rates less than 0.001%. Automatic audit logs provide comprehensive documents, in which blockchain-based systems capture 100% access events and enable real-time compliance monitoring. Emergency access procedures ensure availability during critical conditions, with a break-glass protocol to successfully balance safety and clinical requirements in 99.7% emergency scenarios while maintaining full HIPAA compliance (Vidals, G. 2025) with break-glass protocols.

Table 4: Regulatory Challenges and Technical Solutions (Ramachandran, M. 2024; Vidals, G. 2025)

Regulatory Requirement	Blockchain Challenge	Technical Solution
HIPAA Amendment Rights	Immutable blockchain records	Append-only records with versioning systems
Business Associate Agreements	Distributed node operations	Node operator agreements and smart contract BAAs

Publisher: SARC Publisher

Minimum Necessary Disclosure	Complete data transparency	Zero-knowledge proofs and selective disclosure
Technical Safeguards	Novel technology compliance	End-to-end encryption and biometric authentication
Emergency Access Provision	Privacy vs. critical availability	Break-glass protocols with audit trail enforcement

CONCLUSION

Decentralized identity wallets represent a transformative paradigm shift in healthcare information management, fundamentally restructuring the relationship between patients and their medical data through blockchain technology, cryptographic security, and self-sovereign identity frameworks. By implementing hierarchical deterministic wallets with BIP39 standards, distributed ledger technologies like Hedera Hashgraph, and hybrid storage architectures with zero-knowledge proofs, these systems successfully address critical challenges, including data fragmentation, security vulnerabilities, and limited patient control while maintaining HIPAA compliance. The demonstrated benefits across patient-controlled health records, streamlined administrative workflows, cross-border care, and clinical research, combined with innovative solutions such as append-only record-keeping and smart contract-based governance, effectively bridge blockchain capabilities with healthcare regulatory requirements. As adoption grows and technology matures, decentralized identity solutions will continue to enhance security, operational efficiency, and patient empowerment, ushering in a new era of patient-centric, secure, and interoperable healthcare data management that maintains alignment with critical regulatory standards.

REFERENCES

1. HelixBeat, "The True Cost of Fragmented Healthcare Data." (2025).
2. Kathrin “Kat” Zaki, Christina Hultsch, W. Clifford Mull, “Annual Report to Congress on Breaches of Unsecured Protected Health Information." *Benesch Law.* (2024).
3. Identity Management Institute, "Blockchain for Healthcare Data Security."
4. Minango, J., Carvajal Mora, H., Zambrano, M., Orozco Garzón, N., & Pérez, F. "Distributed Ledger Technology in Healthcare: Enhancing Governance and Performance in a Decentralized Ecosystem." *Technologies* 13.2 (2025): 58.
5. Andrew, J., Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y., & Eunice, J. "Blockchain for healthcare systems: Architecture, security challenges, trends and future directions." *Journal of Network and Computer Applications* 215 (2023): 103633.
6. Leslie, R. "Transforming Healthcare Data Privacy Using Zero Knowledge Proofs." *Sedicii Innovations Ltd.,* (2024).
7. Mohsan, S. A. H., Razzaq, A., Ghayyur, S. A. K., Alkahtani, H. K., Al-Kahtani, N., & Mostafa, S. M. "Decentralized patient-centric report and medical image management system based on blockchain technology and the inter-planetary file system." *International Journal of Environmental Research and Public Health* 19.22 (2022): 14641.
8. AbdelSalam, F. M. "Blockchain revolutionizing healthcare industry: A systematic review of blockchain technology benefits and threats." *Perspectives in Health Information Management* 20.3 (2023): 1b.
9. Ramachandran, M. "Ethics of Blockchain by Design: Guiding a Responsible Future for Healthcare Innovation." *Blockchain in Healthcare Today* 7 (2024): 10-30953.
10. Vidals, G. "The Future of Blockchain in Healthcare: Is it HIPAA-Compliant?" *HIPAA Vault Knowledge Center,* (2025).

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:

Kaimal, S. "Decentralized Identity Wallets: Bridging Blockchain and HIPAA Compliance in Healthcare." *Sarcouncil Journal of Engineering and Computer Sciences* 4.9 (2025): pp 277-283.

Publisher: SARC Publisher